

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-212462

(43)Date of publication of application : 06.08.1999

(51)Int.Cl.

G09C 5/00
 G09C 1/00
 H04L 9/32
 H04N 1/387
 H04N 7/167

(21)Application number : 10-013955

(71)Applicant : CANON INC

(22)Date of filing : 27.01.1998

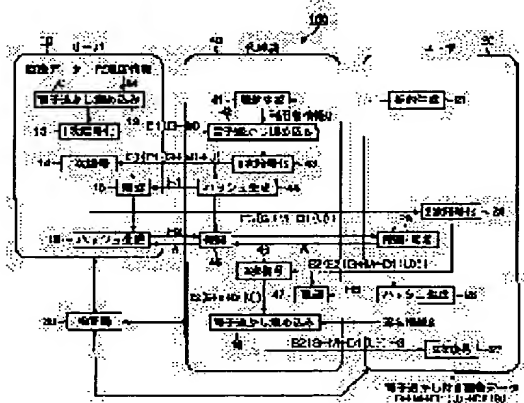
(72)Inventor : IWAMURA KEIICHI

(54) ELECTRONIC WATERMARK SYSTEM, ELECTRONIC INFORMATION DELIVERY SYSTEM, PICTURE FILING DEVICE, AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic information delivery system which surely prevents wrong delivery of data even in the case that elements constituting the purchase and sale of data are hierarchical.

SOLUTION: A first entity 10 subjects original data G to primary encryption processing. A second entity 40 manages and delivers data E1(G+M) after the primary encryption processing and subjects this data to electronic watermark burying processing. A third entity 20 subjects data E3(G+M+D1(U)) after the electronic watermark burying processing to secondary encryption processing.



LEGAL STATUS

[Date of request for examination]

20.05.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-212462

(43)公開日 平成11年(1999)8月6日

(51)Int.Cl. ^a	識別記号	F I	
G 0 9 C	5/00	G 0 9 C	5/00
	1/00		1/00
H 0 4 L	9/32	H 0 4 N	1/387
H 0 4 N	1/387	H 0 4 L	9/00
	7/167	H 0 4 N	7/167
			Z

審査請求 未請求 請求項の数22 O L (全 21 頁)

(21)出願番号 特願平10-13955

(22)出題日 平成10年(1998)1月27日

(71)出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 岩村 恵市

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

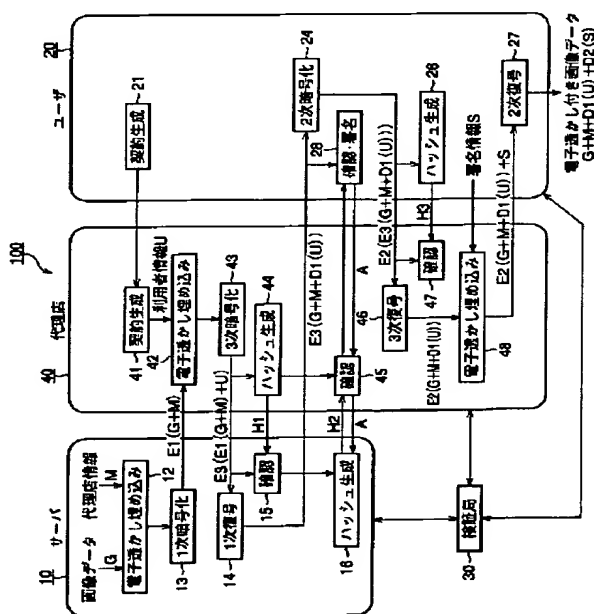
(74) 代理人 弁理士 國分 孝悦

(54) 【発明の名称】 電子透かし方式、電子情報配布システム、画像ファイル装置、及び記憶媒体

(57) 【要約】

【課題】 データの売買を構成する要素が階層的であっても、データの不正配付を確実に防止する電子情報配布システムを提供する。

【解決手段】 第1のエンティティ10は、原データGに1次暗号化処理を行う。第2のエンティティ40は、1次暗号化処理後のデータE1 ($G+M$) を管理及び配布すると共に、それに電子透かし埋込処理を行う。第3のエンティティ20は、電子透かし埋込処理後のデータE3 ($G+M+D1(U)$) に2次暗号化処理を行う。



【特許請求の範囲】

【請求項1】 第1のエンティティが原データに1次暗号化処理を行う第1の工程と、第2のエンティティが上記1次暗号化処理後のデータに少なくとも管理処理及び配布処理の何れかを行うと共に、電子透かし埋込処理を行う第2の工程と、第3のエンティティが上記電子透かし埋込処理後のデータに2次暗号化処理を行う第3の工程とを含むことを特徴とする電子透かし方式。

【請求項2】 上記第1の工程は、上記原データへの1次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う工程を含むことを特徴とする請求項1記載の電子透かし方式。

【請求項3】 上記第2の工程は、上記電子透かし埋込処理の少なくとも前及び後の何れかに、3次暗号化処理を行う工程を含むことを特徴とする請求項1記載の電子透かし方式。

【請求項4】 少なくとも上記1次暗号化処理及び2次暗号化処理の何れかの影響を受け、上記電子透かし埋込処理が行われたデータを配布する工程を更に含むことを特徴とする請求項1記載の電子透かし方式。

【請求項5】 認証局による証明書付き匿名公開鍵によって上記第3のエンティティの署名を検査する工程を更に含むことを特徴とする請求項1記載の電子透かし方式。

【請求項6】 上記第2のエンティティは、複数のエンティティを含むことを特徴とする請求項1記載の電子透かし方式。

【請求項7】 上記第2のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも上記第3のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする請求項1記載の電子透かし方式。

【請求項8】 上記第1の工程は、上記原データへの1次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う工程を含み、

第 n ($n \geq 1$) のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも第 $n+1$ のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする請求項1記載の電子透かし方式。

【請求項9】 上記電子透かし埋込処理は、少なくとも上記第2のエンティティに関する情報を埋め込まない処理であることを特徴とする請求項1又は2に記載の電子透かし方式。

【請求項10】 上記原データは、画像データであることを特徴とする請求項1記載の電子透かし方式。

【請求項11】 少なくとも第1～第3のエンティティを含み、ネットワーク上でのデータの送受信を行う電子情報配布システムであって、

上記第1のエンティティは、原データに1次暗号化処理を行う1次暗号化処理手段を備え、

上記第2のエンティティは、上記1次暗号化処理後のデータに少なくとも管理処理及び配布処理の何れかを行う管理配布処理手段と、電子透かし埋込処理を行う電子透かし埋込処理手段とを備え、

上記第3のエンティティは、上記電子透かし埋込処理後のデータに2次暗号化処理を行う2次暗号化処理手段を備えることを特徴とする電子情報配布システム。

【請求項12】 上記第1のエンティティは、上記原データへの1次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う電子透かし埋込処理手段を更に備えることを特徴とする請求項11記載の電子情報配布システム。

【請求項13】 上記第2のエンティティは、上記電子透かし埋込処理の少なくとも前及び後の何れかに、3次暗号化処理を行う3次暗号化処理手段を更に備えることを特徴とする請求項11記載の電子情報配布システム。

【請求項14】 少なくとも上記1次暗号化処理及び2次暗号化処理の何れかの影響を受け、上記電子透かし埋込処理が行われたデータを配布する配布手段を更に備えることを特徴とする請求項11記載の電子情報配布システム。

【請求項15】 認証局による証明書付き匿名公開鍵によって上記第3のエンティティの署名を検査する検査手段を更に備えることを特徴とする請求項11記載の電子情報配布システム。

【請求項16】 上記第2のエンティティは、複数のエンティティを含むことを特徴とする請求項11記載の電子情報配布システム。

【請求項17】 上記第2のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも上記第3のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする請求項11記載の電子情報配布システム。

【請求項18】 上記第1のエンティティは、上記原データへの1次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う電子透かし埋込処理手段を更に備え、

第 n ($n \geq 1$) のエンティティの上記電子透かし埋込処理手段は、上記電子透かし埋込処理により埋め込む情報を、少なくとも第 $n+1$ のエンティティに関する情報及び送信するデータに関する情報の何れかとして、上記電子透かし埋込処理を行うことを特徴とする請求項11記載の電子情報配布システム。

【請求項19】 上記電子透かし埋込処理手段は、少なくとも上記第2のエンティティに関する情報を埋め込まない上記電子透かし埋込処理を行うことを特徴とする請求項11又は12に記載の電子情報配布システム。

【請求項20】 上記原データは、画像データであるこ

とを特徴とする請求項1記載の電子情報配布システム。

【請求項21】 請求項1～請求項10の何れかに記載の電子透かし方式の各工程で発生するデータを格納することを特徴とする画像ファイル装置。

【請求項22】 請求項1～請求項10の何れかに記載の電子透かし方式の各工程をコンピュータが読出可能に格納したことを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子透かし方式、電子情報配布システム、画像ファイル装置、及び上記電子透かし方式を実施するための工程をコンピュータが読出可能に格納した記憶媒体に関するものであり、特に、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等のデジタル情報における著作権を保護するための電子透かし方式、それを用いてデジタル情報の配布を行うマルチメディアネットワークシステム等の電子情報配布システム、上記電子透かし方式を用いた画像ファイル装置、及び上記電子透かし方式を実施するための工程をコンピュータが読出可能に格納した記憶媒体に関するものである。

【0002】

【従来の技術】近年のコンピュータネットワークの発達と、安価で高性能なコンピュータの普及とにより、ネットワーク上で商品の売買を行う電子商取引が盛んになってきている。そこで取引される商品としては、例えば画像等を含むデジタルデータが考えられる。しかし、デジタルデータは、完全なコピーを容易かつ大量に作成できるという性質を持ち、これは、そのデジタルデータを買ったユーザがオリジナルと同質のコピー（不正コピー）を不正に作成して再配布できるという可能性を示す。これにより、本来デジタルデータの著作者又は著作者から正当に販売を委託された者（以下、「販売者」と言う）に支払われるべき代価が支払われず、著作権が侵害されていると考えられる。

【0003】一方、著作者又は販売者（以下、上述のデジタルデータを正当に配布する者をまとめて「サーバ」と言う）がユーザにデジタルデータを一度送ってしまうと、上述の不正コピーを完全に防止することはできない。このため、不正コピーを直接防止するのではなく、「電子透かし」と呼ばれる手法が提案されている。この「電子透かし」とは、オリジナルのデジタルデータにある操作を加え、デジタルデータに関する著作権情報やユーザに関する利用者情報をデジタルデータ中に埋め込むことによって、不正コピーが見つかった場合に誰がデータを再配布したのかを特定する手法である。

【0004】従来の電子透かしを用いたシステムでは、サーバは完全に信頼できる機関であることが前提となっている。よって、もしサーバが信頼できる機関ではなく

不正を行う可能性があるとする、従来のシステムでは不正コピーを行っていないユーザに罪が押し付けられてしまう場合が存在する。

【0005】これは、図12に示すように、従来のシステムでは、ユーザを特定するための利用者情報d1をデジタルデータ（以下、デジタルデータを画像データとして説明する）gにサーバが埋め込むので、サーバが勝手に利用者情報d1を埋め込んでそのコピーを不正に配布した場合、その利用者情報d1から特定されるユーザは、サーバの主張を退ける手段がないためである。

【0006】その対策として、例えば、「B.Pfitmann and M.Waidner: "Asymmetric Fingerprinting," EUROCR YPT'96」の文献（以下、文献1と言う）に、公開鍵暗号方式を用いたシステム（図13）が提案されている。

【0007】ここで、公開鍵暗号方式とは、暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。その代表例として、RSA暗号やElGamal暗号等が知られている。以下、公開鍵暗号方式における（a）特徴、（b）秘密通信や認証通信等のプロトコルについて述べる。

【0008】（a）公開鍵暗号の特徴

（1）暗号鍵と復号鍵とが異なり、暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

（2）各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

（3）送られてきた通信文の送信者が偽者でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【0009】（b）公開鍵暗号のプロトコル

例えば、通信文Mに対して、公開の暗号鍵kpを用いて行う暗号化操作をE(kp, M)とし、秘密の復号鍵ksを用いて行う復号操作をD(ks, M)とすると、公開鍵暗号アルゴリズムは、まず次の2つの条件を満たす。

（1）暗号鍵kpが与えられたとき、暗号化操作E(kp, M)の計算は容易である。また、復号鍵ksが与えられたとき、復号操作D(ks, M)の計算は容易である。

（2）もしユーザが復号鍵ksを知らないなら、暗号鍵kpと、暗号化操作E(kp, M)の計算手順と、暗号文C=E(kp, M)とを知っていても、通信文Mを決定することは計算量の点で困難である。

【0010】つぎに、上記（1）、（2）の条件に加えて、次の（3）の条件が成立することにより秘密通信機能を実現できる。

（3）全ての通信文（平文）Mに対し暗号化操作E(kp, M)が定義でき、

$$D(ks, E(kp, M)) = M$$

が成立する。つまり、暗号鍵kpは公開されているた

め、誰もが暗号化操作 $E(k_p, M)$ の計算を行うことができるが、 $D(k_s, E(k_p, M))$ の計算をして通信文 M を得ることができるのは、秘密の復号鍵 k_s を持っている本人だけである。

【0011】一方、上記(1)、(2)の条件に加えて、次の(4)の条件が成立することにより認証通信機能を実現できる。

(4) 全ての通信文(平文) M に対し復号操作 $D(k_s, M)$ が定義でき、
 $E(k_p, D(k_s, M)) = M$
 が成立する。つまり、復号操作 $D(k_s, M)$ の計算ができるのは秘密の復号鍵 k_s を持っている本人のみであり、他の人が偽の秘密の復号鍵 k_s' を用いて $D(k_s', M)$ の計算を行い、秘密の復号鍵 k_s を持っている本人になりすましたとしても、
 $E(k_p, D(k_s', M)) \neq M$
 であるため、受信者は受けとった情報が不正なものであることを確認できる。また、 $D(k_s, M)$ の値が改ざんされても、
 $E(k_p, D(k_s, M)') \neq M$
 となり、受信者は受けとった情報が不正なものであることを確認できる。

【0012】上述のような公開鍵暗号方式では、公開の暗号鍵(以下、公開鍵とも言う) k_p を用いる処理 E を「暗号化」、秘密の復号鍵(以下、秘密鍵とも言う) k_s を用いる処理 D を「復号」と呼んでいる。したがって、秘密通信では送信者が暗号化を行い、その後受信者が復号を行なうが、認証通信では送信者が復号を行い、その後受信者が暗号化を行うことになる。

【0013】以下に、公開鍵暗号方式により送信者 A から受信者 B へ秘密通信、認証通信、署名付秘密通信を行う場合のプロトコルを示す。ここで、送信者 A の秘密鍵を $k_s A$ 、公開鍵を $k_p A$ とし、受信者 B の秘密鍵を $k_s B$ 、公開鍵を $k_p B$ とする。

【0014】[秘密通信]送信者 A から受信者 B へ通信文(平文) M を秘密通信する場合は、次の手順で行う。

Step1: 送信者 A は、受信者 B の公開鍵 $k_p B$ で通信文 M を以下のように暗号化し、暗号文 C を受信者 B に送る。

$C = E(k_p B, M)$

Step2: 受信者 B は自分の秘密鍵 $k_s B$ で暗号文 C を以下のように復号し、もとの平文 M を得る。

$M = D(k_s B, C)$

尚、受信者 B の公開鍵 $k_p B$ は不特定多数に公開されているので、送信者 A に限らず全ての人が受信者 B に秘密通信できる。

【0015】[認証通信]送信者 A から受信者 B へ通信文(平文) M を認証通信する場合は、次の手順で行う。

Step1: 送信者 A は、自分の秘密鍵 $k_s A$ で送信文 S を以下のように生成し、受信者 B に送る。

$S = D(k_s A, M)$

この送信文 S を「署名文」と言い、署名文 S を得る操作を「署名」と言う。

Step2: 受信者 B は、送信者 A の公開鍵 $k_p A$ で署名文 S を以下のように復元変換し、もとの平文 M を得る。

$M = E(k_p A, S)$

もし、通信文 M が意味のある文であることを確認したならば、通信文 M が確かに送信者 A から送られてきたことを認証する。送信者 A の公開鍵 $k_p A$ は不特定多数に公開されているので、受信者 B に限らず全ての人が送信者 A の署名文 S を認証できる。このような認証を「デジタル署名」とも言う。

【0016】[署名付秘密通信]送信者 A から受信者 B へ通信文(平文) M を署名付秘密通信する場合は、次の手順で行う。

Step1: 送信者 A は、自分の秘密鍵 $k_s A$ で通信文 M を以下のように署名し、署名文 S を作る。

$S = D(k_s A, M)$

さらに、送信者 A は、受信者 B の公開鍵 $k_p B$ で署名文 S を以下のように暗号化し、暗号文 C を受信者 B に送る。

$C = E(k_p B, S)$

Step2: 受信者 B は、自分の秘密鍵 $k_s B$ で暗号文 C を以下のように復号し、署名文 S を得る。

$S = D(k_s B, C)$

さらに、受信者 B は、送信者 A の公開鍵 $k_p A$ で署名文 S を以下のように復元変換し、もとの平文 M を得る。

$M = E(k_p A, S)$

もし、通信文 M が意味のある文であることを確認したならば、通信文 M が確かに送信者 A から送られてきたことを認証する。

【0017】尚、署名付秘密通信の各Step内における関数を施す順序は、それぞれ逆転しても良い。すなわち、上述の手順では、

Step1: $C = E(k_p B, D(k_s A, M))$

Step2: $M = E(k_p A, D(k_s B, C))$

となっているが、下記のような手順でも署名付秘密通信が実現できる。

Step1: $C = D(k_s A, E(k_p B, M))$

Step2: $M = D(k_s B, E(k_p A, C))$

【0018】そこで、上述のような公開鍵暗号方式を適用した従来の電子透かしを用いるシステム(上記図13)における操作の手順を示す。

【0019】1) 先ず、サーバとユーザ間で画像データ g の売買に関する契約書 $d2$ を取り交わす。

【0020】2) 次に、ユーザは、自分を示す乱数 I を発生させ、これを用いて一方向性関数 f を生成する。この一方向性関数とは、関数 $y = f(x)$ において、 x から y を求めることは容易だが、逆に y から x を求めることが困難な関数を言う。例えば、桁数の大きな整数に

対する素因数分解や離散的対数等が一方方向性関数としてよく用いられる。

3) 次に、ユーザは、契約書 d_2 と一方方向性関数 f に対して、自分の秘密鍵 ks_u を用いて署名情報 d_3 を生成し、それらを合わせてサーバに送る。

【0021】4) 次に、サーバは、ユーザの公開鍵 kp_u を用いて署名情報 d_3 と契約書 d_2 を確認する。

5) サーバは確認後、現在までの全配布記録 d_4 と、ユーザが作成した乱数 ID とを画像データ g に埋め込み、電子透かし付き画像データ $(g + d_4 + ID)$ を生成する。

6) サーバは、ユーザにその電子透かし付き画像データ $(g + d_4 + ID)$ を送る。

【0022】この後、不正コピーが発見された場合は、その不正画像データから埋め込み情報を抽出し、そこに含まれる ID からユーザを特定する。このとき、その不正コピーがサーバによって無断で配布されたものでないことは、以下のことを根拠として主張される。それは、ユーザを特定する ID はユーザ自身によって生成され、それを用いた一方方向性関数値 f にユーザの署名が付けられるので、サーバは任意のユーザに対してそのような ID を生成できないということである。しかし、サーバとの間で正式に契約したユーザは自分を特定する ID をサーバに送るために、正式に契約したユーザへの罪の押し付けはやはり可能であり、契約していないユーザへの罪の押し付けが不可能になるだけである。

【0023】そこで、正式に契約したユーザにも罪の押し付けが不可能になるシステム(図14)が、「三浦、渡辺、嵩(奈良先端大): “サーバの不正も考慮した電子透かしについて”, SCIS97-31C」の文献(以下、文献2と言う)に提案されている。これは、サーバを原画像サーバと埋め込みサーバに分割することによって実現される。ただし、このシステムでは、暗号化時及び復号時において、埋め込まれた電子透かしは壊されないとしている。以下、上記図14のシステムにおける操作の手順を示す。

【0024】1) 先ず、ユーザが原画像サーバに画像データを、署名 d_5 を付けて要求する。

【0025】2) 原画像サーバは、その要求内容をユーザの署名 d_5 から確認し、その確認後に、要求された画像データ g を暗号化して埋め込みサーバに送る。この時、原画像サーバは、ユーザ名 u 及び委託内容 d_6 に対する署名を付けて埋め込みサーバに送る。これと同時に、原画像サーバは、暗号化に対する復号関数 f' をユーザに送る。

【0026】3) 埋め込みサーバは、送られてきた暗号化画像データ g' と、署名 $(u + d_6)$ とを確認し、ユーザ名 u 及び委託内容 d_6 を基にユーザを特定する利用者情報 d_7 の作成及び埋め込みを行い、電子透かし付き暗号化画像データ $(g' + d_7)$ を作成する。その後、

埋め込みサーバは、その電子透かし付き暗号化画像データ $(g' + d_7)$ をユーザに送る。

【0027】4) ユーザは、原画像サーバから送られてきた復号関数 f' を用いて、電子透かし付き暗号化画像データ $(g' + d_7)$ を電子透かし付き画像データ $(g + d_7)$ へと復号する。

【0028】この後、不正コピーが発見された場合は、原画像サーバはその不正画像データを暗号化して埋め込み情報を抽出し、それを埋め込みサーバに送る。埋め込みサーバは、この埋め込み情報からユーザを特定する。このシステムでは、原画像サーバはユーザを特定するための利用者情報 d_7 を画像データ g に埋め込んでおらず、また、埋め込みサーバは復号関数 f' を知らない(画像を元に戻せない)ので、正式に契約したユーザに対しても、各サーバはユーザの利用者情報 d_7 を無断で埋め込んだ画像データ g を不正配布できないことを根拠にしている。

【0029】

【発明が解決しようとする課題】しかしながら、この図14のシステムでは、原画像サーバと埋め込みサーバとの結託については考慮せず、埋め込みサーバとユーザとの結託も考えていない。よって、原画像サーバと埋め込みサーバとが結託した場合には、埋め込みサーバが原画像である画像データ g の暗号化画像データ g' を持ち、ユーザが復号関数 f' を持つため、上述の図13のシステムと同様にサーバの不正が可能であるし、埋め込みサーバとユーザとが結託した場合には、原画像 (g) の不正入手が可能である。

【0030】また、原画像サーバは復号関数 f' をユーザに送るが、ユーザの復号関数 f' の管理が不十分であれば、埋め込みサーバはユーザと結託しなくてもユーザの不注意等から復号関数 f' を知ることができる可能性は大きい。

【0031】さらに、このシステムでは、原画像サーバは埋め込み手段を有しない、或いは正しい埋め込みができないとしているが、埋め込み情報を抽出するのは原画像サーバであるので、埋め込み情報を解析すれば、原画像サーバが正しい埋め込みを行えるようになる可能性は高いと考えられる。これは、埋め込みサーバは自分の署名などを埋め込まないので、埋め込み情報と利用者情報の対応のみが埋め込みサーバの秘密であるが、データベース等を用いた埋め込み情報と利用者情報のランダムな対応ではなく、ある規則に基づいて利用者情報から埋め込み情報が作成される場合、解析される危険性は大きいからである。そして、この場合、上述の図13のシステムと同様の不正が可能である。

【0032】さらにまた、従来より、上述したように、ユーザとサーバからなるシステムは不完全ながら提案されてきたが、サーバが階層的に構成されたシステムでの安全性は保証されていなかった。これは、例えば、図1

5に示すように、サーバの下に複数の販売代理店1、
 ・ ・ ・、mがあり、その下に各々複数のユーザ11、
 ・ ・ ・、1n、
 ・ ・ ・、m1、
 ・ ・ ・、mnがあるといった階層型のシステム（階層型ネットワーク1）や、図16に示すように、複数の著作者1、2、
 ・ ・ ・、m-1、mが属している販売代理店に、ある著作者が自分の画像データの販売を依頼し、その販売代理店が複数の著作者1、2、
 ・ ・ ・、m-1、mの画像データを多くのユーザ1、2、
 ・ ・ ・、nに販売するといった階層型のシステム（階層型ネットワーク2）等では、データの売買を構成する要素が、上述したサーバとユーザの2者からサーバ（又は著作者）と代理店とユーザの3者に増すため、結託の問題等により2者の構成でなるシステムよりもその問題が複雑になるためである。尚、上記図14に示したシステムは、広く考えると、サーバと代理店とユーザの3者の構成でなるシステムとも見れるが、上述の文献2に記載のシステムは、ここで言う階層的なシステムを想定したものではなく、1つのサーバの不正を防止するという観点からサーバを分割したものであり、上述したように、結託の問題も考慮されていないものである。

【0033】そこで、本発明は、上記の欠点を除去するために成されたもので、データの売買を構成する要素が階層的であっても、データの不正配付を確実に防止する電子透かし方式、電子情報配布システム、画像ファイル装置、及び記憶媒体を提供することを目的とする。

【0034】

【課題を解決するための手段】第1の発明は、第1のエンティティが原データに1次暗号化処理を行う第1の工程と、第2のエンティティが上記1次暗号化処理後のデータに少なくとも管理処理及び配布処理の何れかを行うと共に、電子透かし埋込処理を行う第2の工程と、第3のエンティティが上記電子透かし埋込処理後のデータに2次暗号化処理を行う第3の工程とを含む電子透かし方式であることを特徴とする。

【0035】第2の発明は、上記第1の発明において、上記第1の工程は、上記原データへの1次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う工程を含むことを特徴とする。

【0036】第3の発明は、上記第1の発明において、上記第2の工程は、上記電子透かし埋込処理の少なくとも前及び後の何れかに、3次暗号化処理を行う工程を含むことを特徴とする。

【0037】第4の発明は、上記第1の発明において、少なくとも上記1次暗号化処理及び2次暗号化処理の何れかの影響を受け、上記電子透かし埋込処理が行われたデータを配布する工程を更に含むことを特徴とする。

【0038】第5の発明は、上記第1の発明において、認証局による証明書付き匿名公開鍵によって上記第3のエンティティの署名を検査する工程を更に含むことを特

徴とする。

【0039】第6の発明は、上記第1の発明において、上記第2のエンティティは、複数のエンティティを含むことを特徴とする。

【0040】第7の発明は、上記第1の発明において、上記第2のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも上記第3のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする。

【0041】第8の発明は、上記第1の発明において、上記第1の工程は、上記原データへの1次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う工程を含み、第n（ $n \geq 1$ ）のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも第n+1のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする。

【0042】第9の発明は、上記第1又は2の発明において、上記電子透かし埋込処理は、少なくとも上記第2のエンティティに関する情報を埋め込まない処理であることを特徴とする。

【0043】第10の発明は、上記第1の発明において、上記原データは、画像データであることを特徴とする。

【0044】第11の発明は、少なくとも第1～第3のエンティティを含み、ネットワーク上でのデータの送受信を行う電子情報配布システムであって、上記第1のエンティティは、原データに1次暗号化処理を行う1次暗号化処理手段を備え、上記第2のエンティティは、上記1次暗号化処理後のデータに少なくとも管理処理及び配布処理の何れかを行う管理配布処理手段と、電子透かし埋込処理を行う電子透かし埋込処理手段とを備え、上記第3のエンティティは、上記電子透かし埋込処理後のデータに2次暗号化処理を行う2次暗号化処理手段を備える電子情報配布システムであることを特徴とする。

【0045】第12の発明は、上記第11の発明において、上記第1のエンティティは、上記原データへの1次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う電子透かし埋込処理手段を更に備えることを特徴とする。

【0046】第13の発明は、上記第11の発明において、上記第2のエンティティは、上記電子透かし埋込処理の少なくとも前及び後の何れかに、3次暗号化処理を行う3次暗号化処理手段を更に備えることを特徴とする。

【0047】第14の発明は、上記第11の発明において、少なくとも上記1次暗号化処理及び2次暗号化処理の何れかの影響を受け、上記電子透かし埋込処理が行われたデータを配布する配布手段を更に備えることを特徴とする。

【0048】第15の発明は、上記第11の発明におい

て、認証局による証明書付き匿名公開鍵によって上記第3のエンティティの署名を検査する検査手段を更に備えることを特徴とする。

【0049】第16の発明は、上記第11の発明において、上記第2のエンティティは、複数のエンティティを含むことを特徴とする。

【0050】第17の発明は、上記第11の発明において、上記第2のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも上記第3のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする。

【0051】第18の発明は、上記第11の発明において、上記第1のエンティティは、上記原データへの1次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う電子透かし埋込処理手段を更に備え、第 n ($n \geq 1$)のエンティティの上記電子透かし埋込処理手段は、上記電子透かし埋込処理により埋め込む情報を、少なくとも第 $n+1$ のエンティティに関する情報及び送信するデータに関する情報の何れかとして、上記電子透かし埋込処理を行うことを特徴とする。

【0052】第19の発明は、上記第11又は12の発明において、上記電子透かし埋込処理手段は、少なくとも上記第2のエンティティに関する情報を埋め込まない上記電子透かし埋込処理を行うことを特徴とする。

【0053】第20の発明は、上記第11の発明において、上記原データは、画像データであることを特徴とする。

【0054】第21の発明は、請求項1～請求項10の何れかに記載の電子透かし方式の各工程で発生するデータを格納する画像ファイル装置であることを特徴とする。

【0055】第22の発明は、請求項1～請求項10の何れかに記載の電子透かし方式の各工程をコンピュータが読出可能に格納した記憶媒体であることを特徴とする。

【0056】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。

【0057】(第1の実施の形態)

【0058】本発明は、例えば、上記図15に示したような階層型のシステム(代理店が多数にあるシステム)に適用される。図1は、説明の簡単のために、上記図15のシステムにおいて、複数の代理店のうちの任意の代理店に着目して、サーバ、代理店、及び代理店に属する複数のユーザのうちの任意のユーザの構成を簡略化して示したものである。以下、この図1を用いて、本システム100について具体的に説明する。

【0059】システム100は、サーバ(又は著作権等)側の端末装置(サーバ端末装置)10、代理店側の端末装置(代理店端末装置)40、及びユーザ側の端末

装置(ユーザ端末装置)20を含む多数のエンティティ(図示せず)からなるネットワークシステムであり、各エンティティは、ネットワークを介して互いにデジタルデータの授受を行うようになされている。

【0060】サーバ端末装置10は、ユーザ端末装置20からのデータが供給される契約確認処理部11と、例えば画像データ(デジタルデータ)G及び代理店情報Mが供給される電子透かし埋込処理部12と、電子透かし埋込処理部12の出力が供給される1次暗号化処理部13と、代理店端末装置40からのデータが供給される1次復号処理部14と、代理店端末装置40からのデータが供給される確認処理部15と、1次復号処理部14の出力が供給されるハッシュ生成処理部16とを備えている。そして、1次暗号化処理部13及びハッシュ生成処理部16の各出力は、代理店端末装置40に供給されるようになされている。また、1次復号処理部14の出力は、ハッシュ生成処理部16に供給されると共に、代理店端末装置40を介してユーザ端末装置20にも供給されるようになされている。

【0061】代理店端末装置40は、ユーザ端末装置20からのデータが供給される契約生成処理部41と、契約生成処理部41及びサーバ端末装置10の1次暗号化処理部13の各出力が供給される電子透かし埋込処理部42と、電子透かし埋込処理部42の出力が供給される3次暗号化処理部43と、3次暗号化処理部43の出力が供給されるハッシュ生成処理部44と、ハッシュ生成処理部44の出力が供給される確認処理部45と、ユーザ端末装置20からのデータが供給される3次復号処理部46及び確認処理部47と、3次復号化処理部46の出力が供給される電子透かし埋込処理部48とを備えている。そして、3次暗号化処理部43の出力は、ハッシュ生成処理部44に供給されると共に、サーバ端末装置10の1次復号処理部14及び確認処理部15にも供給されるようになされている。また、確認処理部45には、サーバ端末装置10のハッシュ生成処理部16の出力も供給され、確認処理部45の出力は、ユーザ端末装置20にも供給されるようになされている。さらに、電子透かし埋込処理部48には、ユーザ端末装置20からのデータも供給され、電子透かし埋込処理部48の出力は、ユーザ端末装置20に供給されるようになされている。

【0062】ユーザ端末装置20は、代理店端末装置40の契約生成処理部41に対してデータ供給する契約生成処理部21と、サーバ端末装置の1次復号処理部14からのデータが代理店端末装置40を介して供給される2次暗号化処理部24及び確認・署名処理部28と、2次暗号化処理部24の出力が供給されるハッシュ生成処理部26と、代理店端末装置40の電子透かし埋込処理部48の出力が供給される2次復号処理部27とを備えている。そして、2次暗号化処理部24の出力は、ハッ

シュ生成処理部26に供給されると共に、代理店端末装置40の3次復号処理部46及び確認処理部47にも供給されるようになされている。また、ハッシュ生成処理部26の出力は、代理店端末装置40の確認処理部47に供給されるようになされている。さらに、確認・署名処理部28には、代理店端末装置40の確認処理部45の出力が供給されるようになされている。

【0063】上述のようなシステム100では、方式や秘密鍵等の1次暗号に関する情報はサーバだけが知る情報であり、2次暗号に関する情報はユーザだけが知る情報であり、3次暗号に関する情報は代理店だけが知る情報である。ただし、これらの暗号の間には、どちらの暗号化を先に行っても復号を行うとその暗号は解かれる、という性質を持つものとする。以下、暗号化を「 $E_i()$ 」、復号を「 $D_i()$ 」で表わし、電子透かしに関する埋め込み処理を「 $+$ 」で表わすものとする。

【0064】そこで、まず、システム100における電子透かしに関する埋め込み処理について説明する。

【0065】[埋め込み処理]

1) 先ず、ユーザ端末装置20において、ユーザが署名を付けて代理店に画像データを要求する。この要求データは、契約生成処理部21により生成された情報(ユーザの署名情報)であり、以後、これを契約情報と呼ぶ。そして、代理店端末装置40において、ユーザからの契約情報を受け、これを確認した後、画像データをサーバ側に要求する。

【0066】2) 次に、サーバ端末装置10において、電子透かし埋込処理部12は、代理店側から要求された画像データGに代理店情報Mを埋め込む。そして、1次暗号化処理部13は、電子透かし埋込処理部12で代理店情報Mが埋め込まれた画像データ(G+M)を1次暗号化E1して、代理店側に送信する。よって、代理店端末装置40には、1次暗号化画像データE1(G+M)の情報が送られることになる。

【0067】3) 次に、代理店端末装置40において、契約生成処理部41は、ユーザ側からの契約情報から利用者情報Uを生成する。そして、電子透かし埋込処理部42は、契約生成処理部41で生成された利用者情報Uを、サーバ側からの1次暗号化画像データE1(G+M)に埋め込む。3次暗号化処理部43は、電子透かし埋込処理部42で利用者情報Uが埋め込まれた1次暗号化画像データE1(G+M)+Uを3次暗号化E3して、そのデータ(3次暗号化画像データ)E3(E1(G+M)+U)を、サーバ側に送信する。これと同時に、ハッシュ生成処理部44は、送信データ(3次暗号化画像データ)E3(E1(G+M)+U)に対するハッシュ値H1を生成及び署名し、それらをサーバ側に送信する。よって、サーバ端末装置10には、3次暗号化画像データE3(E1(G+M)+U)と、ハッシュ値H1及びその署名が送られることになる。

【0068】尚、上述のハッシュ値とは、一般にハッシュ関数 $h()$ の出力値であり、ハッシュ関数とは衝突を起こしにくい圧縮関数をいう。ここで、衝突とは、異なる値 x_1 、 x_2 に対して $h(x_1)=h(x_2)$ となることである。また、圧縮関数とは、任意のビット長のビット列をある長さのビット列に変換する関数である。したがって、ハッシュ関数とは、任意のビット長のビット列をある長さのビット列に変換する関数 $h()$ で、 $h(x_1)=h(x_2)$ を満たす値 x_1 、 x_2 を容易に見出せないものである。このとき、任意の値 y から $y=h(x)$ を満たす値 x を容易に見出せないで、必然的にハッシュ関数は一方向性関数となる。このハッシュ関数の具体例としては、MD(Message Digest)5やSHA(Secure Hash Algorithm)等が知られている。

【0069】4) 次に、サーバ端末装置10において、確認処理部15は、代理店側からのハッシュ値H1の署名と、そのハッシュ値H1の値が送信データ(3次暗号化画像データE3(E1(G+M)+U))のハッシュ値と一致することを確認し、確認後送られてきたデータを保存する。また、1次復号処理部14は、代理店側からの3次暗号化画像データE3(E1(G+M)+U)の1次暗号化を復号してユーザ代理店側に送信する。これと同時に、ハッシュ生成処理部16は、送信データ(E3(G+M+D1(U)))に対するハッシュ値H2を生成及び署名し、それらを代理店側に送信する。よって、代理店端末装置40には、データE3(G+M+D1(U))と、ハッシュ値H2及びその署名とが送られることになる。

【0070】5) 次に、代理店端末装置40において、確認処理部45は、サーバ側からのハッシュ値H2の署名と、そのハッシュ値H2が送信データ(E3(G+M+D1(U)))のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、確認処理部45は、サーバ側からのデータをそのままユーザ側に送信する。よって、ユーザ端末装置20には、データE3(G+M+D1(U))と、ハッシュ値H2及びその署名とが送られることになる。

【0071】6) 次に、ユーザ端末装置20において、確認・署名処理部28は、代理店側からのハッシュ値H2の署名と、そのハッシュ値H2が送信データ(E3(G+M+D1(U)))のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、確認・署名処理部28は、ハッシュ値H2に自分の署名Aを生成して、代理店を介してサーバ側に送信する。そして、代理店端末装置40の確認処理部45、及びサーバ端末装置10のハッシュ生成処理16は各々、ユーザ側からの署名Aを確認し、その確認後それを保存する。

【0072】7) 次に、ユーザ端末装置20において、2次暗号化処理部24は、代理店側からのデータE3

($G+M+D1(U)$)を2次暗号化 $E2$ して、それを代理店側に送信する。これと同時に、ハッシュ生成処理部26は、送信データ($E2(E3(G+M+D1(U)))$)に対するハッシュ値 $H3$ を生成及び署名し、それらを代理店側に送信する。また、自分の証明情報 S を生成して、それを代理店側に送信する。よって、代理店端末装置40には、データ $E2(E3(G+M+D1(U)))$ と、ハッシュ値 $H3$ 及びその署名と、証明情報 S とが送られることになる。

【0073】8)次に、代理店端末装置40において、確認処理部47は、ユーザ側からのハッシュ値 $H3$ の署名と、そのハッシュ値 $H3$ が送信データ($E2(E3(G+M+D1(U)))$)のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、3次復号処理部46は、ユーザ側からのデータ $E2(E3(G+M+D1(U)))$ の3次暗号を復号する。そして、電子透かし埋込処理部48は、ユーザ側からの証明情報 S を、3次復号処理部46で復号して得られたデータ $E2(G+M+D1(U))$ に埋め込み、そのデータ $E2(G+M+D1(U))+S$ をユーザ側に送信する。また、ハッシュ生成処理部49は、このデータ $E2(G+M+D1(U))$ のハッシュ値 $H4$ を生成し、そのハッシュ値 $H4$ に署名してユーザ側に送信する。よって、ユーザ端末装置20には、データ $E2(G+M+D1(U))+S$ が送られることになる。

【0074】9)次に、ユーザ端末装置20において、確認処理部29は、代理店側からのハッシュ値 $H4$ の署名を確認すると共に、このハッシュ値 $H4$ がデータ $E2(G+M+D1(U))$ のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。そして、2次復号処理部27は、代理店側からのデータ $E2(G+M+D1(U))+S$ の2次暗号を復号し、電子透かし付き画像データ G_w を取り出して出力する。この画像データ G_w は、 $G_w = G+M+D1(U)+D2(S)$

で表せる。これは、元の画像データ G に対して、代理店情報 M と、1次復号を受けた利用者情報(透かし情報) U と、2次暗号の影響を受けた署名情報 S とが埋め込まれていることを示す。

【0075】以上のことから、ユーザの署名情報 S の埋め込みは代理店側で行われるため、ユーザは基本的に不正することはできない。また、代理店は、ユーザの利用者情報 U 及び署名情報 S の埋め込みを行うが、利用者情報 U は、サーバのみが知る1次暗号の影響を受け、署名情報 S は、ユーザのみが知る2次暗号化の影響を受けるため、代理店は、 $D1(U+D2(S))$ を直接元の画像データ G に埋め込むことはできない。このとき、不正コピー(不正画像)が発見された場合、例えば、図2に示すフローチャートに従った手順で不正ユーザの特定を行う(以下、これを検証処理と言う)。ただし、ここで

は、上述の文献1、文献2と同様に、画像データは透かし情報の変形及び消去を受けないものとする。

【0076】[検証処理]

1) 先ず、サーバは、発見した不正画像データ G_w' から代理店情報 M' を抽出する(ステップS101)。このとき、代理店情報 M' が抽出されなかった場合、サーバ(又は著作者等)の不正と認定する(ステップS102)。これは、代理店情報 M' の埋め込みを行ったのはサーバ側であるためである。

【0077】2) 1)にて、正しい代理店情報 M が抽出された場合($M'=M$ の場合)、サーバは、検証局30に不正画像データ G_w' 及び1次暗号化の鍵を提出し、不正画像データ G_w' の1次暗号化(ステップS103)と利用者情報 U' の抽出(ステップS104)を要求する。このとき、正しい利用者情報 U' が抽出された場合($U'=U$ の場合)、後述する8)に進む。

【0078】3) 2)にて、正しい利用者情報 U' が抽出されなかった場合、検証局30は、サーバに対して、保存しているデータ $E3(E1(G+M)+U)$ と、ハッシュ値 $H1$ 及びその署名とを要求し、ハッシュ値 $H1$ 及びその署名を確認する。その後、検証局30は、データ $E3(E1(G+M)+U)$ の1次暗号を復号し、そのハッシュ値を生成し、そのハッシュ値が代理店が保存しているハッシュ値 $H2$ と一致することを確認する。また、これと同時に、検証局30は、ハッシュ値 $H2$ の署名検査も行う(ステップS105)。

【0079】4) 3)にて、検証局30にて生成されたハッシュ値と、代理店が保存しているハッシュ値 $H2$ とが一致しなかった場合、検証局30は、サーバの不正と認定する(ステップS106)。これは、サーバが提出した1次暗号の鍵が正しくないことを意味するからである。

【0080】5) 3)にて、検証局30にて生成されたハッシュ値と、代理店が保存しているハッシュ値 $H2$ とが一致した場合、検証局30は、代理店に3次暗号の鍵の提出を要求し、サーバが保存していたデータ $E3(E1(G+M)+U)$ の3次暗号を復号して利用者情報 U' を抽出する(ステップS107)。

【0081】6) 5)にて、正しい利用者情報 U' が抽出された場合($U'=U$ の場合)、検証局30は、サーバの不正と認定する(ステップS108)。これは、利用者情報 U' の埋め込み処理が正当に行われたことを意味するからである。また、5)までの検証処理によって、不正画像データ G_w' の1次暗号が正しく、利用者情報 U' が不正であることが示されたため、この不正画像データ G_w' を生成できるのは1次暗号を知るサーバのみであるからである。

【0082】7) 5)にて、正しい利用者情報 U' が抽出されなかった場合、検証局30は、代理店の不正と認定する(ステップS109)。これは、埋め込み処理

において、正しい利用者情報U'が埋め込められなかったことを意味し、また、この利用者情報U'の埋め込みは代理店側で行われるからである。

【0083】8) 上述の2)にて、正しい利用者情報U'が抽出された場合(U'=Uの場合)、検証局30は、サーバと代理店に対して、保存されているハッシュ値H2と、ユーザによるハッシュ値H2の署名A'との提出を要求し、その署名A'を確認する(ステップS110)。

【0084】9) 8)にて、正しい署名A'が確認されなかった場合(提出されなかった場合)、検証局30は、サーバと代理店の結託による不正と認定する(ステップS111)。これは、サーバと代理店が結託して、任意のユーザ(利用者情報U')を示すデータG+M+D1(U')を偽造したことを意味するからである。

【0085】10) 8)にて、正しい署名A'が確認された場合(A'=Aの場合)、検証局30は、ユーザに対して、2次暗号の鍵の提出を要求し、不正画像データGw'の2次暗号化を行い(ステップS112)、署名情報S'の抽出を行う(ステップS113)。

【0086】11) 10)にて、正しい署名情報S'が抽出された場合(S'=Sの場合)、検証局30は、ユーザの不正と認定する(ステップS114)。これは、2次暗号化して署名情報S'に戻す処理は、ユーザ側で行えないからである。

【0087】12) 10)にて、正しい署名情報S'が抽出されなかった場合、検証局30は、ユーザに対して、保存されているデータE3(G+M+D1(U))と、ハッシュ値H3及びその署名の提出を要求し、ハッシュ値H3及びその署名を確認する。その後、検証局30は、データE3(G+M+D1(U))の2次暗号化を行うと共に、そのハッシュ値を生成し、それがハッシュ値H3と一致することを確認する。これと同時に、検証局30は、ハッシュ値H3の署名検査も行う(ステップS115)。

【0088】13) 12)にて、検証局30で生成されたハッシュ値と、ユーザが保存しているハッシュ値H3とが一致しない場合、検証局30は、ユーザの不正と認定する(ステップS116)。これは、ユーザが提出した2次暗号の鍵が正しくないことを意味するからである。

【0089】14) 12)にて、検証局30で生成されたハッシュ値と、ユーザが保存しているハッシュ値H3とが一致した場合、検証局30は、代理店の不正と認定する(ステップS117)。これは、埋め込み処理において、代理店が正しく署名情報Sを埋め込まなかったことを意味するからである。

【0090】以上のことにより、本実施の形態によれば、検証局30は不正画像が発見されるまで必要なく、不正画像が発見される以前に不正を行うことはできな

い。また、上述の検証処理の手順が公知で、サーバと代理店とユーザが互いにその結果を見届け合うならば、検証局30がなくても、状況に応じて各自の不正を特定することができる。

【0091】(第2の実施の形態)

【0092】本発明は、例えば、上記図16に示したような階層型のシステム(代理店が1つのシステム)に適用される。図3は、説明の簡単のために、上記図16のシステムにおいて、複数の著作者(又はサーバ等)代理店及び複数のユーザのうちの任意の著作者及びユーザに着目して、著作者(ここでは、サーバとして説明する)、代理店、及びユーザの構成を簡略化して示したものである。以下、この図3を用いて、本システム200について具体的に説明する。

【0093】システム200は、上記図1に示したシステム100と同様の構成としているが、次の点が異なっている。

1) サーバ端末装置10において、電子透かし埋込処理部12は設けられておらず、1次暗号化処理部13に画像データGのみが供給される。

2) 代理店端末装置40において、電子透かし埋込処理部48の出力が供給されるハッシュ生成処理部49が更に設けられており、このハッシュ生成処理部49の出力は、ユーザ端末装置20に供給される。

3) ユーザ端末装置20において、代理店端末装置40の電子透かし埋込処理部48及びハッシュ生成処理部49の各出力が供給される確認処理部29が更に設けられている。

【0094】上述のように、システム200では、代理店を示す代理店情報Mの埋め込みを省略した構成としている。そこで、まず、システム200における電子透かしに関する埋め込み処理について説明する。

【0095】尚、上記図3のシステム200において、上記図1のシステム100と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略する。

【0096】[埋め込み処理]

1) 先ず、ユーザ端末装置20において、ユーザが署名を付けて代理店に画像データ(契約情報)を要求する。そして、代理店端末装置40において、ユーザからの契約情報を受け、これを確認した後、画像データをサーバ側に要求する。

【0097】2) 次に、サーバ端末装置10において、1次暗号化処理部13は、画像データGを1次暗号化E1して、代理店側に送信する。よって、代理店端末装置40には、1次暗号化画像データE1(G)が送られることになる。

【0098】3) 次に、代理店端末装置40において、契約生成処理部41は、ユーザ側からの契約情報から利用者情報Uを生成する。そして、電子透かし埋込処理部42は、契約生成処理部41で生成された利用者情報U

を、サーバ側からの1次暗号化画像データE1(G)に埋め込む。3次暗号化処理部43は、電子透かし埋込処理部42で利用者情報Uが埋め込まれた1次暗号化画像データE1(G)+Uを3次暗号化E3して、そのデータ(3次暗号化画像データ)E3(E1(G)+U)を、サーバ側に送信する。これと同時に、ハッシュ生成処理部44は、送信データ(3次暗号化画像データ)E3(E1(G)+U)に対するハッシュ値H1を生成及び署名し、それらをサーバ側に送信する。よって、サーバ端末装置10には、3次暗号化画像データE3(E1(G)+U)と、ハッシュ値H1及びその署名が送られることになる。

【0099】4)次に、サーバ端末装置10において、確認処理部15は、代理店側からのハッシュ値H1の署名と、そのハッシュ値H1の値が送信データ(3次暗号化画像データE3(E1(G)+U))のハッシュ値と一致することを確認し、確認後送られてきたデータを保存する。また、1次復号処理部14は、代理店側からの3次暗号化画像データE3(E1(G)+U)の1次暗号化を復号してユーザ代理店側に送信する。これと同時に、ハッシュ生成処理部16は、送信データ(E3(G+D1(U)))に対するハッシュ値H2を生成及び署名し、それらを代理店側に送信する。よって、代理店端末装置40には、データE3(G+D1(U))と、ハッシュ値H2及びその署名とが送られることになる。

【0100】5)次に、代理店端末装置40において、確認処理部45は、サーバ側からのハッシュ値H2の署名と、そのハッシュ値H2が送信データ(E3(G+D1(U)))のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、確認処理部45は、サーバ側からのデータをそのままユーザ側に送信する。よって、ユーザ端末装置20には、データE3(G+D1(U))と、ハッシュ値H2及びその署名とが送られることになる。

【0101】6)次に、ユーザ端末装置20において、確認・署名処理部28は、代理店側からのハッシュ値H2の署名と、そのハッシュ値H2が送信データ(E3(G+D1(U)))のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、確認・署名処理部28は、ハッシュ値H2に自分の署名Aを生成して、代理店を介してサーバ側に送信する。そして、代理店端末装置40の確認処理部45、及びサーバ端末装置10のハッシュ生成処理16は各々、ユーザ側からの署名Aを確認し、その確認後それを保存する。

【0102】7)次に、ユーザ端末装置20において、2次暗号化処理部24は、代理店側からのデータE3(G+D1(U))を2次暗号化E2して、それを代理店側に送信する。これと同時に、ハッシュ生成処理部26は、送信データ(E2(E3(G+D1(U))))

に対するハッシュ値H3を生成及び署名し、それらを代理店側に送信する。また、自分の証明情報Sを生成して、それを代理店側に送信する。よって、代理店端末装置40には、データE2(E3(G+D1(U)))と、ハッシュ値H3及びその署名と、証明情報Sとが送られることになる。

【0103】8)次に、代理店端末装置40において、確認処理部47は、ユーザ側からのハッシュ値H3の署名と、そのハッシュ値H3が送信データ(E2(E3(G+D1(U))))のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、3次復号処理部46は、ユーザ側からのデータE2(E3(G+D1(U)))の3次暗号を復号する。そして、電子透かし埋込処理部48は、ユーザ側からの証明情報Sを、3次復号処理部46で復号して得られたデータE2(G+D1(U))+Sをユーザ側に送信する。よって、ユーザ端末装置20には、データE2(G+D1(U))+Sが送られることになる。

【0104】9)次に、ユーザ端末装置20において、2次復号処理部27は、代理店側からのデータE2(G+D1(U))+Sの2次暗号を復号し、電子透かし付き画像データGwを取り出して出力する。この画像データGwは、

$$G_w = G + D1(U) + D2(S)$$

で表せる。これは、元の画像データGに対して、1次復号を受けた利用者情報(透かし情報)Uと、2次暗号の影響を受けた署名情報Sとが埋め込まれていることを示す。

【0105】以上のことから、ユーザの署名情報Sの埋め込みは代理店側で行われるため、ユーザは基本的に不正することはできない。また、代理店は、ユーザの利用者情報U及び署名情報Sの埋め込みを行うが、利用者情報Uは、サーバのみが知る1次暗号の影響を受け、署名情報Sは、ユーザのみが知る2次暗号化の影響を受けるため、代理店は、D1(U+D2(S))を直接元の画像データGに埋め込むことはできない。このとき、不正コピー(不正画像)が発見された場合、以下の手順で検証処理を行うことで、上述した代理店情報Mを用いず、不正した代理店を特定できるようになされている。ただし、ここでは、上述の文献1、文献2と同様に、画像データは透かし情報の変形及び消去を受けないものとする。

【0106】[検証処理]

1) 先ず、サーバは、検証局30に対して、発見した不正画像データGw'から1次暗号の鍵を提出し、不正画像データGw'の1次暗号化と利用者情報U'の抽出を要求する。正しい利用者情報U'が抽出された場合(U'=Uの場合)、後述する7)に進む。

【0107】2) 1)にて、正しい利用者情報U'が抽

出されなかった場合、検証局30は、サーバに対して、保存しているデータE3 ($E1(G) + U$) と、ハッシュ値H1及びその署名とを要求し、ハッシュ値H1及びその署名を確認する。その後、検証局30は、データE3 ($E1(G) + U$) の1次暗号を復号し、そのハッシュ値を生成し、そのハッシュ値が代理店が保存しているハッシュ値H2と一致することを確認する。また、これと同時に、検証局30は、ハッシュ値H2の署名検査も行う。

【0108】3) 2) にて、検証局30にて生成されたハッシュ値と、代理店が保存しているハッシュ値H2とが一致しなかった場合、検証局30は、サーバの不正と認定する。これは、サーバが提出した1次暗号の鍵が正しくないことを意味するからである。

【0109】4) 2) にて、検証局30にて生成されたハッシュ値と、代理店が保存しているハッシュ値H2とが一致した場合、検証局30は、代理店に3次暗号の鍵の提出を要求し、サーバが保存していたデータE3 ($E1(G) + U$) の3次暗号を復号して利用者情報U' を抽出する。

【0110】5) 4) にて、正しい利用者情報U' が抽出された場合 ($U' = U$ の場合)、検証局30は、サーバの不正と認定する。これは、利用者情報U' の埋め込み処理が正当に行われたことを意味するからである。また、4) までの検証処理によって、不正画像データGw' の1次暗号が正しく、利用者情報U' が不正であることが示されたため、この不正画像データGw' を生成できるは1次暗号を知るサーバのみであるからである。

【0111】6) 4) にて、正しい利用者情報U' が抽出されなかった場合、検証局30は、代理店の不正と認定する。これは、埋め込み処理において、正しい利用者情報U' が埋め込まれなかったことを意味し、また、この利用者情報U' の埋め込みは代理店側で行われるからである。

【0112】7) 上述の1) にて、正しい利用者情報U' が抽出された場合 ($U' = U$ の場合)、検証局30は、サーバと代理店に対して、保存されているハッシュ値H2と、ユーザによるハッシュ値H2の署名A' との提出を要求し、その署名A' を確認する。

【0113】8) 7) にて、正しい署名A' が確認されなかった場合 (提出されなかった場合)、検証局30は、サーバと代理店の結託による不正と認定する。これは、サーバと代理店が結託して、任意のユーザ (利用者情報U') を示すデータG+D1 (U') を偽造したことを意味するからである。

【0114】9) 7) にて、正しい署名A' が確認された場合 ($A' = A$ の場合)、検証局30は、ユーザに対して、2次暗号の鍵の提出を要求し、不正画像データGw' の2次暗号化を行い、署名情報S' の抽出を行う。

【0115】10) 9) にて、正しい署名情報S' が抽

出された場合 ($S' = S$ の場合)、検証局30は、ユーザの不正と認定する (ステップS114)。これは、2次暗号化して署名情報S' に戻す処理は、ユーザ側で行えないからである。

【0116】11) 9) にて、正しい署名情報S' が抽出されなかった場合、検証局30は、ユーザに対して、保存されているデータE3 ($G+D1(U)$) と、ハッシュ値H3及びその署名の提出を要求し、ハッシュ値H3及びその署名を確認する。その後、検証局30は、データE3 ($G+D1(U)$) の2次暗号化を行うと共に、そのハッシュ値を生成し、それがハッシュ値H3と一致することを確認する。これと同時に、検証局30は、ハッシュ値H3の署名検査も行う。

【0117】12) 11) にて、検証局30で生成されたハッシュ値と、ユーザが保存しているハッシュ値H3とが一致しない場合、検証局30は、ユーザの不正と認定する。これは、ユーザが提出した2次暗号の鍵が正しくないことを意味するからである。

【0118】13) 11) にて、検証局30で生成されたハッシュ値と、ユーザが保存しているハッシュ値H3とが一致した場合、検証局30は、代理店の不正と認定する。これは、埋め込み処理において、代理店が正しく署名情報Sを埋め込まなかったことを意味するからである。

【0119】以上のことにより、本実施の形態によっても、検証局30は不正画像が発見されるまで必要なく、不正画像が発見される以前に不正を行うことはできない。また、上述の検証処理の手順が公知で、サーバと代理店とユーザが互いにその結果を見届け合うならば、検証局30がなくても、状況に応じて各自の不正を特定することができる。

【0120】(第3の実施の形態)

【0121】まず、近年において、電子現金と呼ばれるネットワーク上の通貨が実現されつつある。この電子現金は、通常の現金と同様に所有者の名前が記されないで匿名性が実現されている。もし、匿名性が実現されない場合、商品の売り手は、電子現金から誰がどの商品を購入したかという情報を知ることができ、ユーザのプライバシーが犯されることになるからである。このため、電子透かしによる著作権の著作権保護と同様に、ユーザのプライバシー保護の実現は重要である。

【0122】そこで、この第3の実施の形態では、購入時にはユーザの匿名性が実現され、画像の不正配布のような不正が発見されたときには、電子透かしの本来の目的である不正配布者の特定が行えるようにする。これは、例えば、図4に示すようなシステム300により実現される。

【0123】このシステム300は、上記図3のシステム200と同様の構成としているが、ユーザ端末装置20には、認証局40からの匿名公開鍵証明書が与えられ

る構成としている。

【0124】ここで、通常、署名情報を検査する公開鍵には、その正当性を証明するために認証局とよばれる機関による証明書が付されていることが多い。この認証局とは、公開鍵暗号方式におけるユーザの公開鍵の正当性を保証するために、ユーザの公開鍵に証明書を発行する機関を言う。すなわち、認証局は、ユーザの公開鍵やユーザに関するデータに認証局の秘密鍵で署名を施すことによって証明書を作成し、発行する。あるユーザから自分の証明書付き公開鍵を送られた他のユーザは、この証明書を認証局の公開鍵で検査することによって、公開鍵を送ってきたユーザの正当性（少なくとも、認証局によって認められたユーザであるということ）を認証する。このような認証局を運営している組織として、VeriSignやCyberTrustという企業がよく知られている。

【0125】よって、上述した第2の実施の形態における埋め込み処理の1)において、代理店がユーザの契約情報を署名から確認する場合、認証局の証明書付きの公開鍵で確認することが考えられる。しかし、この証明書には通常、公開鍵の所有者の名前が記されている。よってこの場合、データの購入時におけるユーザの匿名性は実現されていないことになる。

【0126】これに対して、公開鍵と所有者の対応を認証局が秘密に保持することも、公開鍵の証明書に所有者の名前を記さないこともできる。このような証明書付きの公開鍵を、以後「証明書付き匿名公開鍵」と呼ぶ。

【0127】そこで、ユーザは、上述した第2の実施の形態における埋め込み処理の1)において、契約情報と一緒に契約情報の署名、及び署名情報Sを検査する証明書付き匿名公開鍵を送れば、ユーザは購入時に自分を匿名にすることができる。よって、代理店には、利用者を特定する情報として証明書付き匿名公開鍵が渡されるが、不正発見時にはその証明書付き匿名公開鍵を認証局50に示して、その公開鍵に対応するユーザを教えることによって、ユーザを特定できる。

【0128】以上のことから、上述した第2の実施の形態における埋め込み処理の1)と、その検証処理の7)を以下のようにすることによって、ユーザの購入時の匿名性と不正発見時の不正者特定が実現される。

【0129】以下、上記図4のシステム300における埋め込み処理、及び検証処理について具体的に説明する。

【0130】尚、上記図4のシステム300において、上記図3のシステム200と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略し、異なる部分についてののみ具体的に説明するものとする。また、埋め込み処理の1)と、その検証処理の1)以外については、上述した第2の実施の形態と同様であるため、その詳細な説明は省略する。

【0131】[埋め込み処理]

1') 先ず、ユーザ端末装置20において、契約生成処理部21は、認証局50からの証明書付き匿名公開鍵と一緒に、画像データを要求する契約情報をその公開鍵に対応する署名を付けて代理店側に送る。代理店端末装置40において、ユーザ側からの契約情報を証明書付き匿名公開鍵から確認し、その後、画像データをサーバ側に要求する。

【0132】以降、上述した第2の実施の形態における埋め込み処理の2)～9)と同様の処理を行う。

【0133】この場合も、ユーザは基本的に不正することとはできず、また、代理店は、D1(U+D2(S))を直接元の画像データGに埋め込むことはできない。このとき、不正コピー(不正画像)が発見された場合、以下の検証処理を行う。

【0134】[検証処理]1)～6) 先ず、上述した第2の実施の形態における検証処理の1)～6)と同様の処理を行う。

【0135】7') 上述の1)にて、正しい利用者情報U'が抽出された場合(U'=Uの場合)、検証局30は、その利用者情報U'と契約情報から得られる証明書付き匿名公開鍵を認証局50に提出し、認証局50に対して、その証明書付き匿名公開鍵に対応するユーザ名を要求する。また、検証局30は、サーバと代理店に対して、保存しているハッシュ値H2及びユーザによるハッシュ値H2の署名A'の提出を要求し、その署名A'を確認する。

【0136】以降、上述した第2の実施の形態における検証処理の8)～13)と同様の処理を行う。

【0137】以上のことにより、本実施の形態によっても、上述した第2の実施の形態と同様に、検証局30は不正画像が発見されるまで必要なく、不正画像が発見される以前に不正を行うことはできない。また、上述の検証処理の手順が公知で、サーバと代理店とユーザが互いにその結果を見届け合うならば、検証局30がなくても、状況に応じて各自の不正を特定することができる。

【0138】尚、第3の実施の形態では、第2の実施の形態におけるシステム200に認証局50を設けた構成としたが、これに限らず、第1の実施の形態におけるシステム100に認証局50を設けた構成としてもよい。この場合、第1の実施の形態における埋め込み処理の1)が上述の1')となり、第1の実施の形態における検証処理の8)が上述の7')となる。

【0139】上述の第1～び第3の実施の形態に示した画像データ及び透かし情報の埋め込み処理によって得られる各段階のハッシュ値を含む種々のデータは、以下のようなフォーマットで格納することができる。

【0140】例えば、下記の一般的な画像フォーマットでは、各段階で送付される画像データを画像データ部に格納し、それに対応するハッシュ値やその署名などを画像ヘッダ部に格納することができる。また、最終的にユ

ーザが保存しておく必要があるハッシュ値、及びその署名や2次暗号の鍵等を画像ヘッダ部に、電子透かし付き画像データを画像データ部に格納しておくことができる。

【0141】一方、下記に示すFlashPix™ファイルフォーマットでは、上述のようなハッシュ値やその署名を含む一般的な画像フォーマットを各階層のデータとして格納することができる。また、ハッシュ値やその署名等は、属性情報としてプロパティセットの中に格納しておくこともできる。

【0142】[一般的な画像フォーマットの説明] 一般的な画像フォーマットは、図5に示すように、画像ファイルは画像ヘッダ部と画像データ部とに分けられる。一般的に画像ヘッダ部には、その画像ファイルから画像データを読み取る時に必要な情報や、画像の内容を説明する付帯的な情報が格納される。上記図5の例では、その画像フォーマット名を示す画像フォーマット識別子、ファイルサイズ、画像の幅・高さ・深さ、圧縮の有無、解像度、画像データの格納位置へのオフセット、カラーパレットの情報等の情報が格納されている。一方、画像データ部は、画像データを順次格納している部分である。このような画像フォーマットの代表的な例としては、Microsoft 社のBMPフォーマットやCompuserve社のGIFフォーマットなどが広く普及している。

【0143】[FlashPix™ファイルフォーマットの説明] 以後説明するFlashPix™(FlashPixは米国Eastman Kodak 社の登録商標) ファイルフォーマットでは、上記画像ヘッダ部に格納されていた画像属性情報および画像データ部に格納されていた画像データを、更に構造化してファイル内に格納する。この構造化した画像ファイルを、図6及び図7に示す。ファイル内の各プロパティやデータには、MS-DOSのディレクトリとファイルに相当する、ストレージとストリームによってアクセスする。上記図6及び図7において、影付き部分がストレージで、影なし部分がストリームであり、画像データや画像属性情報はストリーム部分に格納される。

【0144】上記図6において、画像データは異なる解像度で階層化されており、それぞれの解像度の画像をSubimageと呼び、Resolution0, 1, . . . , nで示してある。各解像度の画像に対して、その画像データを読み出すために必要な情報がSubimage Header に、また画像データがSubimage data に格納される。

【0145】プロパティセットとは、属性情報をその使用目的や内容に応じて分類して定義したものであり、Summary info. Property Set、Image info. Property Set、Image Content Property Set、Extention list property Set がある。

【0146】[各プロパティセットの説明] Summary info. Property Setは、FlashPix特有のものではなく、Microsoft 社のストラクチャードストレージでは必須のプ

ロパティセットで、そのファイルのタイトル・題名・著者・サムネール画像等を格納する。また、Comp Obj.Stream には、記録部(Strage)に関する一般的な情報が格納される。Image Content Property Setは、画像データの格納方法を記述する属性である(図8参照)。この属性には、画像データの階層数、最大解像度の画像の幅や高さ、それぞれの解像度の画像についての幅、高さ、色の構成、あるいはJPEG圧縮を用いる際の量子化テーブル・ハフマンテーブルの定義などを記述する。Extention list property Set は、上記FlashPixの基本仕様に含まれない情報を追加する際に使用する領域である。更に、ICC Profile の部分には、ICC(International Color Consortium)において規定される色空間変換のための変換プロファイルが記述される。

【0147】また、Image info. Property Setは、画像データを使用する際に利用できる下記のような様々な情報、例えば、その画像がどのようにして取り込まれ、どのように利用可能であるかの情報を格納する。

- ・デジタルデータの取り込み方法/あるいは生成方法に関する情報
- ・著作権に関する情報
- ・画像の内容(画像中の人物、場所など)に関する情報
- ・撮影に使われたカメラに関する情報
- ・撮影時のカメラのセッティング(露出、シャッタースピード、焦点距離、フラッシュ使用の有無など)の情報
- ・デジタルカメラ特有の解像度やモザイクフィルタに関する情報
- ・フィルムのメーカー名、製品名、種類(ネガ/ポジ、カラー/白黒)などの情報
- ・オリジナルが書物や印刷物である場合の種類やサイズに関する情報
- ・スキャン画像の場合、使用したスキャナやソフト、操作した人に関する情報

【0148】上記図7のFlashPix Image View Object は、画像を表示する際に用いるビューイングパラメータと画像データとを合わせて格納する画像ファイルである。ビューイングパラメータとは、画像の回転、拡大/縮小、移動、色変換、フィルタリングの処理を画像表示の際に適応するために記憶しておく処理係数のセットである。この図7において、Global info.property setの部分には、ロックされている属性リストが記述されており、例えば、最大画像のインデックスや最大変更項目のインデックス、最終修正者の情報等が記述される。また、同図において、Source/Result FlashPix Image Object は、FlashPix画像データの実体であり、Source FlashPix Image Objectは必須で、Result FlashPix Image Objectはオプションである。Source FlashPix Image Objectはオリジナルの画像データを、ResultFlashPix Image Objectはビューイングパラメータを使って画像処理した結果の画像データをそれぞれ格納する。

【0149】また、Source/Result desc. Property Setは、上記画像データの識別のためのプロパティセットであり、画像ID、変更禁止のプロパティセット、最終更新日時等を格納する。Transform Property Setは、画像の回転、拡大／縮小、移動のためのAffine変換係数、色変換マトリクス、コントラスト調整値、フィルタリング係数を格納している。

【0150】〔画像データの取り扱いの説明〕ここでは、複数のタイルに分割された複数の解像度の画像を含む画像フォーマットを例に挙げて説明する。

【0151】図9に、解像度の異なる複数の画像から構成される画像ファイルの例を示す。この図9において、最大解像度の画像は列×行が $X0 \times Y0$ で構成されており、その次に解像度の大きい画像は $X0/2 \times Y0/2$ であり、それ以降順次、列・行ともに $1/2$ ずつ縮小し、列・行ともに64画素以下あるいは互いに等しくなるまで縮小されていく。

【0152】このように画像データを階層化した結果、画像の属性情報として「1つの画像ファイル中の階層数」や、それぞれの階層の画像に対して、一般的な画像フォーマットの項で説明したヘッダ情報と画像データとが必要となる（上記図5参照）。1つの画像ファイル中の階層の数や最大解像度の画像の幅、高さ、あるいはそれぞれの解像度の画像の幅、高さ、色構成、圧縮方式等に関する情報は、上記Image Content Property Set中に記述される（上記図8参照）。

【0153】さらに、各解像度のレイヤの画像は、図10に示すように64画素×64画素でなるタイル毎に分割されている。画像の左上部から順次64画素×64画素のタイルに分割をすると、画像によっては右端および下端のタイルの一部に空白が生ずる場合がある。この場合は、それぞれ最右端画像または最下端画像を繰り返し挿入することで、64画素×64画素を構築する。

【0154】FlashPix™では、それぞれのタイル中の画像データをJPEG圧縮、シングルカラー、非圧縮のいずれかの方法で格納する。JPEG圧縮は、ISO/IEC JTC1/SC29により国際標準化された画像圧縮方式であり、方式自体の説明はここでは割愛する。また、シングルカラーとは、上記1つのタイルがすべて同じ色で構成されている場合にのみ、個々の画素の値を記録することなく、そのタイルの色を1色で表現する方式である。この方法は特に、コンピュータグラフィックスにより生成された画像で有効である。

【0155】このようにタイル分割された画像データは、例えば上記図6のSubimage dataストリーム中に格納され、タイルの総数、個々のタイルのサイズ、データの開始位置、圧縮方法はすべてSubimage Headerに格納されている（図11参照）。

【0156】尚、以上に述べた第1～第3の実施の形態において、透かし情報の埋め込みは、種々の手法によ

て実現できるが、例えば、「清水、沼尾、森本（日本IBM）：“ピクセルブロックによる静止画像データハイディング”，情報処理学会第53回全国大会，1N-11，平成8年9月」の文献3や、「I.J.Cox, J.Kilian, T.Leighton and T.shamoon(NEC)：“Secure Spread Spectrum Watermarking for Multimedia,” NEC Research Institute Technical Report 95-10.」の文献4に示されるような公知の埋め込み手法によって実現できる。

【0157】また、1次暗号～3次暗号として用いられる暗号方式も種々の方式によって実現できるが、例えばビットの配置を暗号鍵に応じて換えるといった暗号方式によって実現できる。

【0158】さらに、全ての送信データにハッシュ値とその署名を付けて送ることもできる。

【0159】また、1次暗号～3次暗号は、透かし情報の埋め込み処理において互いの情報を知らせないために用いられるが、第三者からの通信路上での盗聴および改ざんを防ぐために、別にDES(Data Encryption Standard)等の暗号やハッシュ関数等を用いても良い。

【0160】また、上述の第1～第3の実施の形態において、不正配布の検出はサーバ（又は著作権等）側で行っているが、1次暗号又は2次暗号に関する秘密鍵を知らなくても電子透かしの抽出手段さえ持っていれば、誰にでも不正配布および不正配布の利用者情報を知ることができる。その後、不正配布発見をサーバ側に知らせて検証処理を始めさせれば良いので、不正配布の発見者はサーバに限定されない。

【0161】また、サーバ側は、利用者情報Uだけでなく、必要に応じて著作権情報やその画像データの配布状況に関する情報等の他の情報を画像データに埋め込むこともできる。また、サーバ又は代理店側で秘密の情報を埋め込みたい場合は、1次暗号化の後に埋め込み処理を行えば、署名情報と同様に1次暗号の影響を受けた情報を埋め込むことができる。さらに、利用者情報Uは、必ず1次暗号化の前にある必要はなく、1次暗号化の後に埋め込んでよい（この場合、利用者情報Uの検出は、サーバ又は代理店又は1次暗号の秘密鍵を知る者のみが行える）。

【0162】また、ユーザ側が共通のプリンタや端末等を用いる第2のエンティティである場合、ユーザの署名情報及び2次暗号は、プリンタや共通端末の署名情報や暗号方式を含む場合がある。

【0163】また、サーバ（又は著作権等）側の1次暗号化情報は、ユーザ側からの契約情報による依頼がなくても、ネットワークやCD-ROM等によって広く配布されていても良い。

【0164】また、ユーザの署名情報Sは、公開鍵暗号方式によって生成されるものに限らず、ユーザが契約情報等で定めた情報（暗号番号のような情報等）でもよい。

【0165】また、米国では、40ビット以上の暗号を用いる場合、暗号の悪用を防ぐために、暗号鍵を管理する鍵管理局を必要とする。このような場合、検証局30に鍵管理局を兼ねさせることも可能である。よって、検証局30が2次暗号の鍵を予め管理している場合は、不正画像の監視も検証局が行うようにすれば、上述の検証処理1)～3)は検証局30が単独で行うことができる。このとき、サーバの1次暗号の鍵は、同じ検証局によって管理されていてもよいし、異なる他の検証局に管理されていてもよい。また、サーバやユーザの鍵は、鍵管理局が生成し、配付するようにしてもよい。

【0166】また、代理店は、1つは限らず、複数の代理店が階層的に構成されていてもよい。この場合、代理店の行う処理は、階層中の担当代理店が代表して行うようにしてもよいし、代理店間で上述のプロトコルを実行し、責任を明らかにするようにしてもよい。

【0167】また、サーバ(又は著作者等)は、要求された後に元の画像データGの1次暗号のデータE1

(G)又はE1(G+M)を代理店側に送るようにしたが、予めデータE1(G)又はE1(G+M)を代理店側に送るようにしてもよい。

【0168】また、代理店の3次暗号の影響は、最終的に得られる画像データG_Wに残らないが、利用者情報Uの埋め込みを3次暗号化の後に行う、或いは、署名情報Sの埋め込みを3次暗号化の後に行う等を行うことで、3次暗号の影響を残すようにしてもよい。

【0169】また、本発明の目的は、上述した第1～第3の実施の形態のホスト及び端末の機能を実現するための工程をソフトウェアのプログラムコードとして記憶した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ(又はCPUやMPU)が記憶媒体に格納されたプログラムコードを読みだして実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が上述した実施の形態の機能を実現することとなり、そのプログラムコードを記憶した記憶媒体は本発明を構成することとなる。

【0170】プログラムコードを供給するための記憶媒体としては、ROM、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモ리카ード等を用いることができる。

【0171】また、コンピュータが読みだしたプログラムコードを実行することにより、上述した第1～第3の実施の形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOS等が実際の処理の一部又は全部を行い、その処理によって第1～第3の実施の形態の機能が実現される場合も含まれることは言うまでもない。

【0172】さらに、記憶媒体から読み出されたプログ

ラムコードが、コンピュータに挿入された拡張機能ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部又は全部を行い、その処理によって上述した第1～第3の実施の形態の機能が実現される場合も含まれることは言うまでもない。

【0173】

【発明の効果】以上説明したように本発明によれば、第3のエンティティ(ユーザ)に関する情報の埋め込みを第2のエンティティ(代理店等)側で行なうことができる。この場合、第3のエンティティは不正することはいできない。また、第2のエンティティは、第3のエンティティに関する情報(利用者情報Uや署名情報S等)の埋め込みを行うが、その情報は、第1のエンティティ(サーバ又は著作者等)のみが知る暗号(1次暗号化、第1の暗号化手段における暗号)や、第3のエンティティのみが知る暗号(2次暗号化、第2の暗号化手段における暗号)の影響を受けるため、第2のエンティティは、第3のエンティティに関する情報を直接原データに埋め込むことはできない。したがって、階層的に構成されたネットワークにおいても、データの不正配付を確実に防止することができ、安全なシステムが実現できる。また、ユーザの匿名性も容易に実現できる。

【図面の簡単な説明】

【図1】第1の実施の形態において、本発明を適用したシステムの構成を示すブロック図である。

【図2】上記システムでの検証処理を説明するためのフローチャートである。

【図3】第2の実施の形態において、本発明を適用したシステムの構成を示すブロック図である。

【図4】第3の実施の形態において、本発明を適用したシステムの構成を示すブロック図である。

【図5】一般的な画像フォーマットを説明するための図である。

【図6】構造化画像ファイル(1)を説明するための図である。

【図7】構造化画像ファイル(2)を説明するための図である。

【図8】画像データの格納方法を記述する属性を説明するための図である。

【図9】解像度の異なる複数の画像から構成される画像ファイルの一例を説明するための図である。

【図10】各解像度のレイヤの画像を説明するための図である。

【図11】画像データの個々のタイルデータを説明するための図である。

【図12】従来の電子透かしを用いたシステムを説明するための図である。

【図13】上記システムを改良した従来の電子透かしを

20 ユーザ側の端末装置

21 契約生成処理部

24 2次暗号化处理部

26 ハッシュ生成処理部

27 2次復号処理部

28 確認・署名処理部

30 検証局

40 代理店側の端末装置

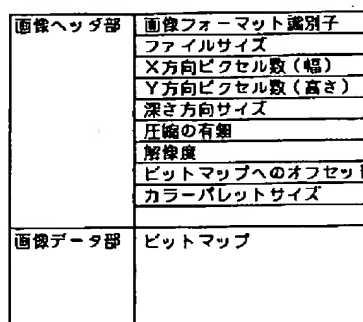
4.1 契約生成処理部

42 電子透かし埋込処理部

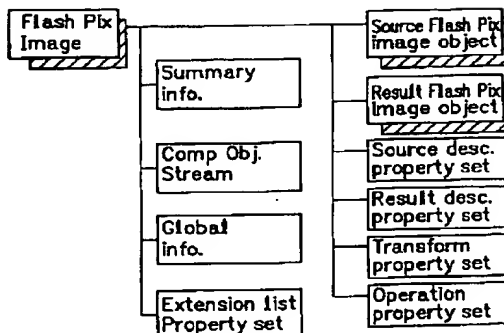
4.3 3次暗号化处理部

44 ハッシュ生成処理部

【図5】



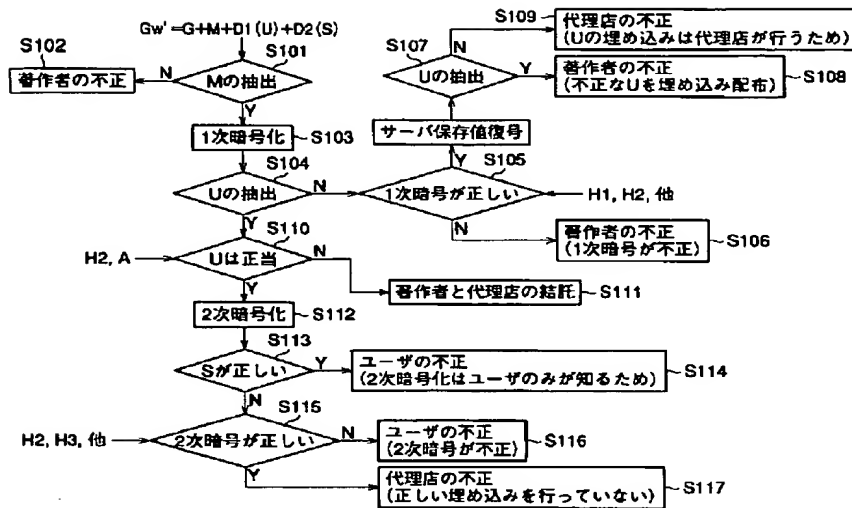
【图7】



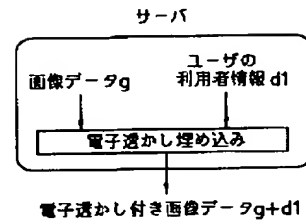
【图 11】

フィールド名	長さ	バイト
画枠の幅	4	4-7
画枠の高さ	4	8-11
タイルの線数	4	12-15
タイルの粗	4	16-19
タイルの高さ	4	20-23

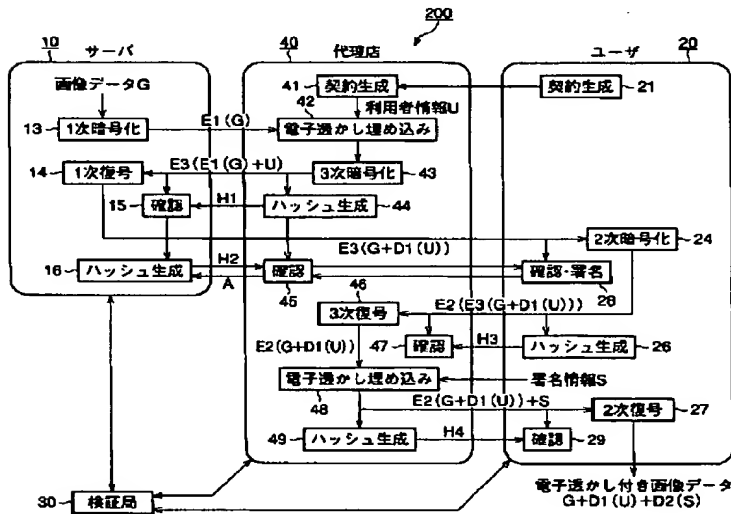
【図2】



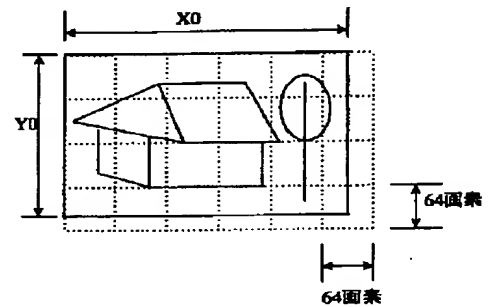
【図12】



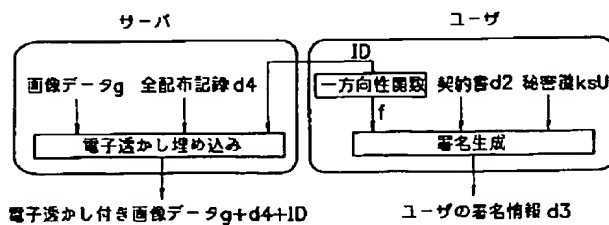
【図3】



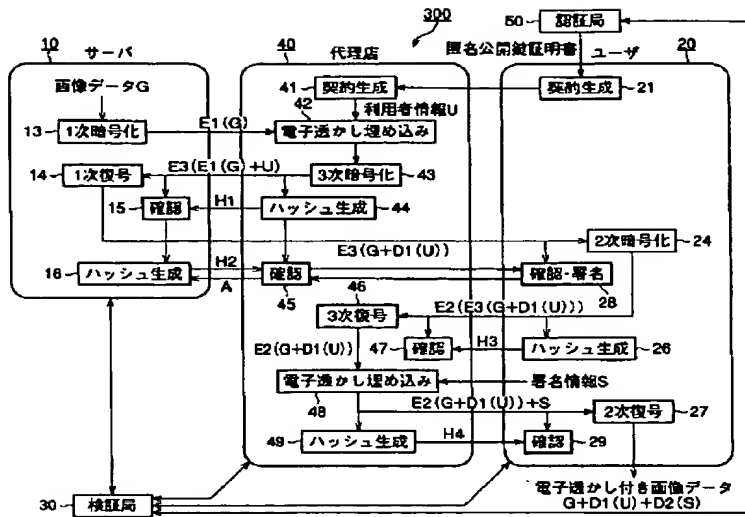
【図10】



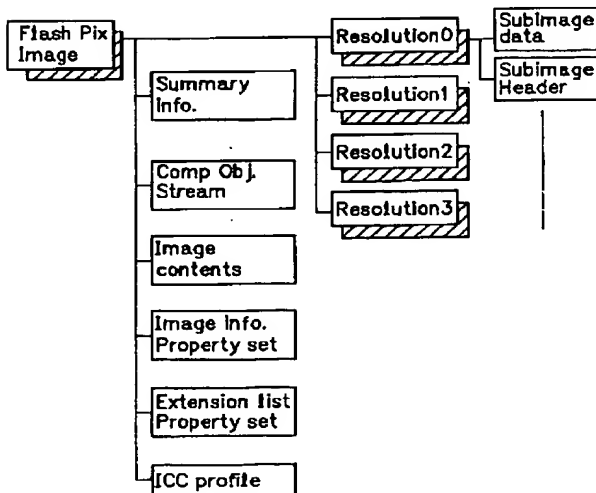
【図13】



【図4】



【図6】



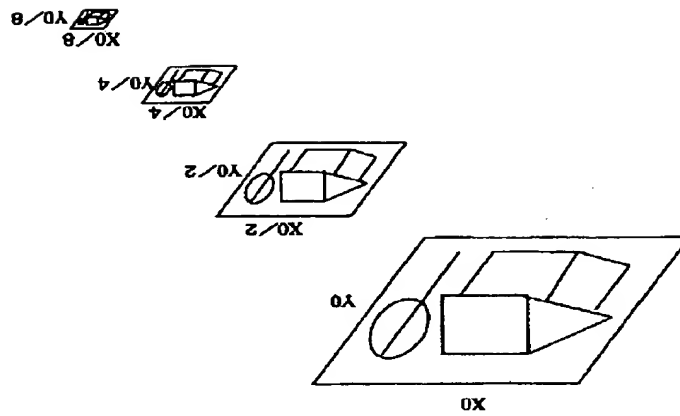
【図8】

プロパティ名	IDコード	タイプ
画像データの階層数	0x01000000	VT_UI4
最大解像度の画像の幅	0x01000002	VT_UI4
最大解像度の画像の高さ	0x01000003	VT_UI4
初期表示の高さ	0x01000004	VT_R4
初期表示の幅	0x01000005	VT_R4

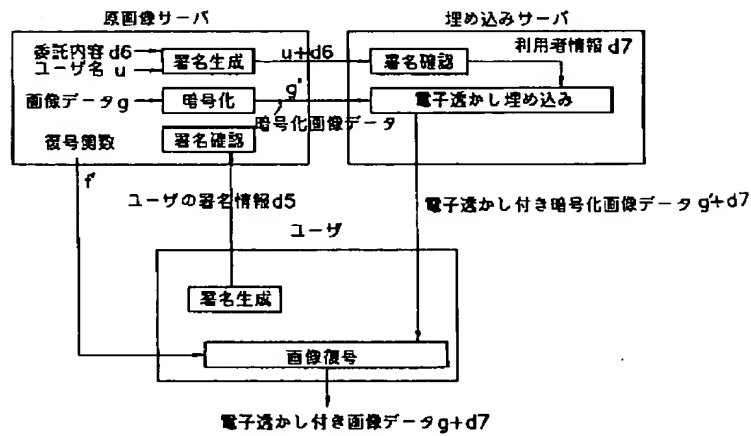
プロパティ名	IDコード	タイプ
各解像度の画像の幅	0x02ii0000	VT_UI4
各解像度の画像の高さ	0x02ii0001	VT_UI4
各解像度の画像の色	0x02ii0002	VT_BLOB
各解像度の画像を数値で表わしたフォーマット	0x02ii0003	VT_UI4 VT_VECTOR

プロパティ名	IDコード	タイプ
JPEGテーブル	0x03ii0001	VT_BLOB
最大JPEGテーブルのインデックス	0x03000002	VT_UI4

【図9】

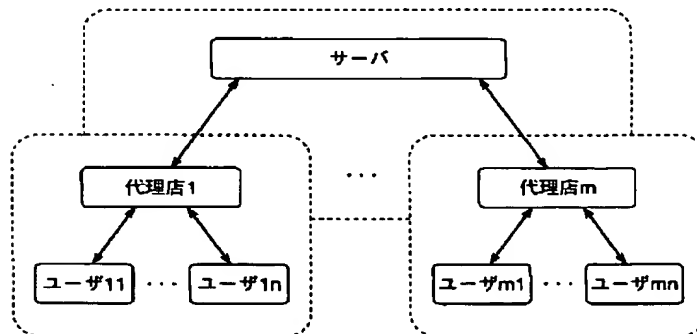


【図14】



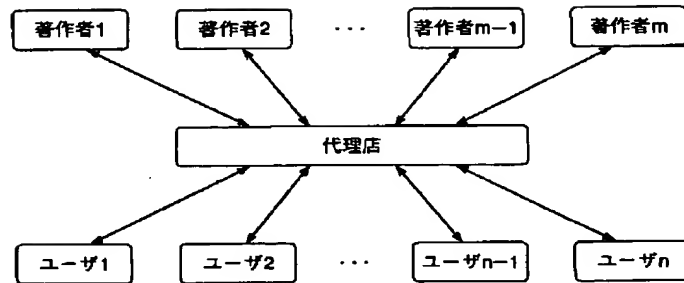
【図15】

・階層型ネットワーク (1)



【図16】

階層型ネットワーク (2)



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.